Amendment Dated August 27, 2007
Serial No. 10/615,513

IN THE CLAIMS

Claim 1. (Previously Presented) An industrial network, comprising:

  a local area network;

  one or more programmable logic controllers; and

  a security policy implementation point (SPIP) connected between the local area network and the one or more programmable logic controllers to isolate the one or more programmable logic controllers and associated factory machines from the local area network, the SPIP being configured to participate in a Virtual Private Network (VPN) such that communications with the SPIP over the industrial network occur over a VPN tunnel.

Claim 2. (Previously Presented) The industrial network of claim 1, wherein the SPIP is integrated with the programmable logic controller and wherein the SPIP is logically connected between the local area network and the one or more programmable logic controllers.

Claim 3. (Previously Presented) The industrial network of claim 1, wherein the network contains a plurality of programmable logic controllers, wherein the one or more programmable logic controllers are a subset of the plurality of programmable logic controllers, and wherein the SPIP is physically disposed between the local area network and the one or more programmable logic controllers.

Claim 4. (Original) The industrial network of claim 3, wherein the local area network is an Ethernet network, wherein the SPIP is configured to communicate with network devices on the local area network over the Ethernet network, and wherein the SPIP is configured to communicate with the programmable logic controller using a protocol selected from at least one of Profibus, Controller Area Network, RS-232, RS-422, and RS-485.

Claim 5. (Original) The industrial network of claim 1, wherein the local area network includes at least one Ethernet switch/router, and wherein the SPIP is included as a blade in the Ethernet switch/router.

-2-

Amendment Dated August 27, 2007
Serial No. 10/615,513

Claim 6. (Original) The industrial network of claim 5, wherein the SPIP is configured to implement security policy to control network access to at least one PLC connected to the Ethernet switch/router through the SPIP.

Claim 7. (Previously Presented) The industrial network of claim 1, wherein the SPIP is further configured to apply policy to limit access to the programmable logic controllers to individuals authorized to access the programmable logic controllers and to require authentication on the SPIP before allowing control instructions to pass from the local area network through the SPIP to the one or more programmable logic controller.

Claim 8. (Canceled)

Claim 9. (Original) The industrial network of claim 1, wherein the industrial network is an untrusted network configured to interconnect network services with a plurality of SPIPs associated with factory machines, and wherein the network services are configured to enable operation of the factory machines to be altered through the industrial network.

Claim 10. (Previously Presented) The industrial network of claim 1, wherein the SPIP is further configured to enable local access to the one or more programmable logic controllers by applying local authentication and authorization policy to enable the SPIP to enforce network policy in connection with attempted local access.

Claim 11. (Original) The industrial network of claim 10, wherein the local policy comprises:
      a local access policy configured to require authentication and authorization of at least one of an user and an accessing electronic device for non-emergency attempts to access the SPIP, and
      an alternate access policy configured to allow access to the SPIP and maintain an audit log attendant to a local attempt to access the SPIP.

Claim 12. (Canceled)

-3-

Amendment Dated August 27, 2007
Serial No. 10/615,513

Claim 13. (Currently Amended) The industrial network of ~~claim 12~~ claim 1, wherein the SPIP comprises a local authentication policy and information associated with authorized users and indicative of authorization policy information associated with said at least one factory machine.

Claim 14. (Previously Presented) A Security Policy Implementation Point (SPIP) for use in an industrial network, comprising:

a local path configured to implement a local access policy related to direct local access to one or more programmable logic controllers; and

a network path connected between the industrial network and the one or more programmable logic controllers to control access to the programmable logic controller via the industrial network, the network path being configured to isolate the one or more programmable logic controllers and associated factory machines from the industrial network by participation in a Virtual Private Network such that communications with the SPIP over the industrial network occur over a VPN tunnel.

Claim 15.   (Currently Amended)   The SPIP of ~~claim 15~~ claim 14, further comprising programmable logic controller circuitry configured to implement the one or more programmable logic controllers and to function to control at least one factory machine.

Claim 16. (Previously Presented) The SPIP of claim 15, wherein the local access policy includes enabling access to an associated factory machine to enable operation of the factory machine to be altered without verification of authorization and authentication of an user seeking to alter the operation during an emergency.

Claim 17. (Original) The SPIP of claim 16, wherein the local path further comprises an accounting module configured to record accesses to at least one of the SPIP, an associated programmable logic controller, and an associated factory machine.

Claim 18. (Original) The SPIP of claim 15, wherein the local path comprises an authentication module configured to authenticate the identity of an individual seeking to access a device

-4-

Amendment Dated August 27, 2007
Serial No. 10/615,513

through the SPIP, and an authorization module configured to assess an authorization associated
with the individual to ascertain whether the individual is authorized to access the device.

Claim 19. (Original) The SPIP of claim 18, wherein the authorization module is an interface to
a Lightweight Directory Access Protocol (LDAP) server, and wherein the authentication module
is an interface to a Remote Access Dial In User Service (RADIUS) server.

Claim 20. (Original) The SPIP of claim 18, wherein the authentication and authorization
modules maintain a local copy of authorized users and authentication policy to allow local access
to the SPIP.

Claim 21. (Previously Presented) The SPIP of claim 15, wherein the SPIP is configured to
apply policy to limit access to the programmable logic controllers to individuals authorized to
access the programmable logic controllers and to require authentication on the SPIP before
allowing control instructions to pass from the industrial network through the SPIP to the one or
more programmable logic controllers.

Claim 22. (Original) The SPIP of claim 15, further comprising network ports configured to
interface with the industrial network, and output ports configured to interface with a
programmable logic controller.

Claim 23. (Original) The SPIP of claim 22, wherein the network ports are configured to
communicate on the industrial network utilizing an Ethernet protocol; and wherein the output
ports are configured to communicate with the programmable logic controller using a protocol
understandable by the programmable logic controller.

Claim 24. (Original) The SPIP of claim 15, further comprising network ports configured to
interface with the industrial network, control logic configured to implement a control program
associated with a programmable logic controller, and interface ports configured to interface with
a factory machine.

-5-

Amendment Dated August 27, 2007
Serial No. 10/615,513

Claim 25. (Original) The SPIP of claim 24, wherein the interface ports comprise at least one input port configured to receive input from an environmental sensor, and at least one output port configured to control at least one electro-mechanical device.

-6-